Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

Enhancing Energy Efficiency in Wireless Sensor Network

Abdul Razak Qureshi[1] , Prof. R.K. Krishna[2]
[1]*Department of Computer Science & Engineerings, Rajiv Gandhi College of Engineering, Research & Technology, Chandrapur-442401(MS)*
[2] *Department of Electronic Rajiv Gandhi College of Engineering, Research & Technology, Chandrapur-442401 (MS)*

Abstract— small embedded devices called sensors in a wireless sensor networks (WSN) which communicate wirelessly with ad-hoc configuration. This paper explores permanent energy drain-out attack at routing protocol layer in wireless sensor network, which causes infected node from network permanently by draining battery power. This Vampire attacks are rely on the properties of classes of routing protocol and not specific to the routing protocol layer. These attacks are difficult to detect and easy to carry out by sending protocol compliant messages to the neighbouring nodes in network. We analyse and compare such attack and energy consumption in AODV routing protocol and suggested method to eliminate such attack.

Keywords— Vampire attack, Wireless Sensor Network attack, WSN, Clustering, Node, Routing.

I. INTRODUCTION

Applications such as continuous connectivity, weather monitoring, industry and instantly -deployable communication for first responders and military. These networks already consider environmental conditions, factory performance, and troop deployment, to name some applications. [1][2] To mitigate network attack problems, there are methods which can stop attacks from happening on the short-term availability of a network but they do not address attacks that affect long term availability. Vampire attack causes denial of service attack is to completely drain energy of sensor node. These attacks work over time to completely disable a network called vampire attack [4] [5].

Vampire attacks are not protocol-specific and they do not depend on design properties or implementation faults of specific routing protocols, but rather exploit properties of protocol classes such as link state, distance-vector, source routing, and geo-graphic and beacon routing. [2][3][4][5]Vampire attacks do not depend on flooding the network with large amounts of data rather try to transmit as little data as possible to get the largest energy drain which prevents a rate limiting solution. Vampires attack use protocol compliant messages which make it very hard to detect and prevent in network [7]. Existing work on securing routing attempts to confirm that intruder cannot cause path discovery to return an invalid network path, but Vampires do not modify routing paths instead of that it uses existing valid network paths and protocol compliant messages which requires normal health check and before actual data transfer over the network [4][6].

Vampire attackers are malicious insider node having the same resources and level of network access as honest nodes. Attacker location within the network is assumed to be fixed and random. This is far from the strongest adversary model; rather this configuration represents the average expected damage from Vampire attacks [6][7]. Smart adversary placement or dynamic node compromise would make attacks far more damaging. In this paper we are exploring energy consumption in AODV routing protocol after Vampire attack and how to enhance the energy of node by detecting and protecting from vampire attack

II. METHODOLOGY

DETECTING VAMPIRE ATTACK

Scan the network with energy consumption level as compare to initial energy. Identify sensor nodes with lowest energy or zero energy and consider as infected node. Monitor abnormal behaviour in network communication and set threshold limit of legitimate message as compare to normal network communication time. While generating vampire attack, attacker node keep sending messages even after communication between nodes are finished. The node which are abnormal in behaviour is considered as attacker. Remove infected nodes and malicious nodes from the network topology for attack free communication. Energy consumption will be less with no malicious nodes in WSN as normal nodes doesn't have to respond to malicious nodes.

IMPLEMENTING LEACH PROTOCOL

In WSN, LEACH save network energy greatly compared with non-cluster algorithm. Many other clustering algorithm are proposed on LEACH such as TEEN (Threshold sensitive Energy Efficient Sensor Network Protocol) [11] PEGASIS (Power Efficient Gathering in Sensor Information Systems) [12] and so on. In LEACH protocol, all clusters are self-organised, each cluster contains a cluster head and several non-cluster nodes. Attacker head consumes more energy than non cluster head nodes. With the purpose of balancing network energy consumption and prolong the network life cycle, it selects cluster head randomly and each node has equal chance to be a cluster head []. Once Cluster Head CH1 is elected, initiate one more round of next Cluster Head CH2 selection process. The node which having less energy or equivalent to CH1 will be elected as CH2. The dual Cluster head in network topology helps in frequent round of cluster head selection and saves node energy. Once the CH1 energy reaches to alarming level, CH2 takes part in active communication and inform all nodes about the Cluster head.

III. SIMULATION RESULTS AND COMPARISON

The prosed system is implemented using NS2 ver 2.34. NS2 is mainly used for simulation purpose where we can configure routing protocol such as AODV. Around 36 nodes are considered to form the Cluster and cluster head selection. The below fig: 1 shows cluster network formation after detecting and eliminating malicious and infected sensor node from network topology formation.

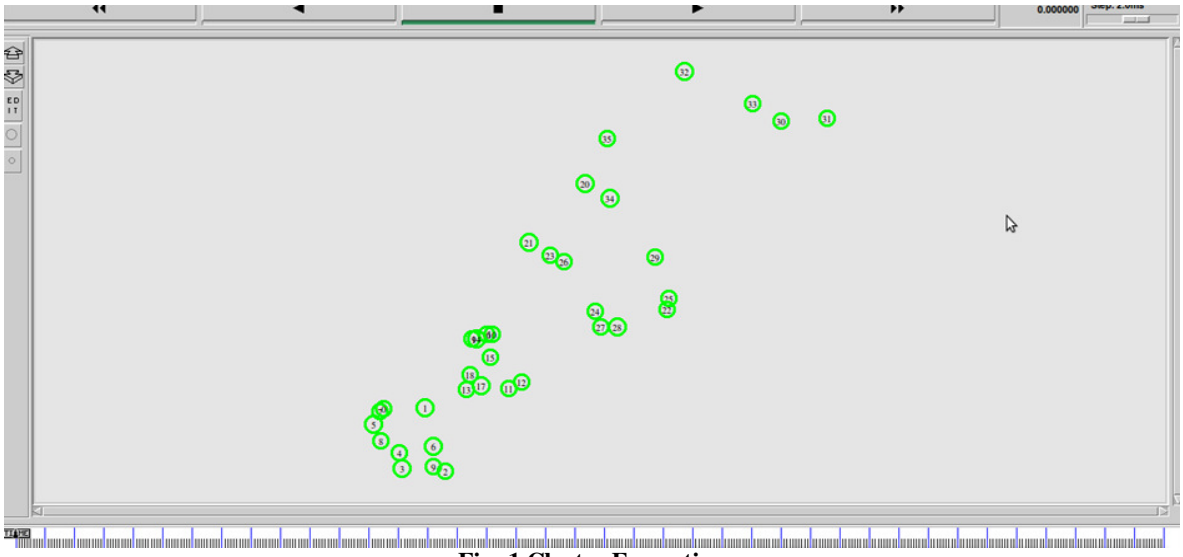

Fig: 1 Cluster Formation

Below fig. 2 shows formation of cluster with cluster head selection CH1 & CH2 and communication. No malicious and infected node is part of network topology.

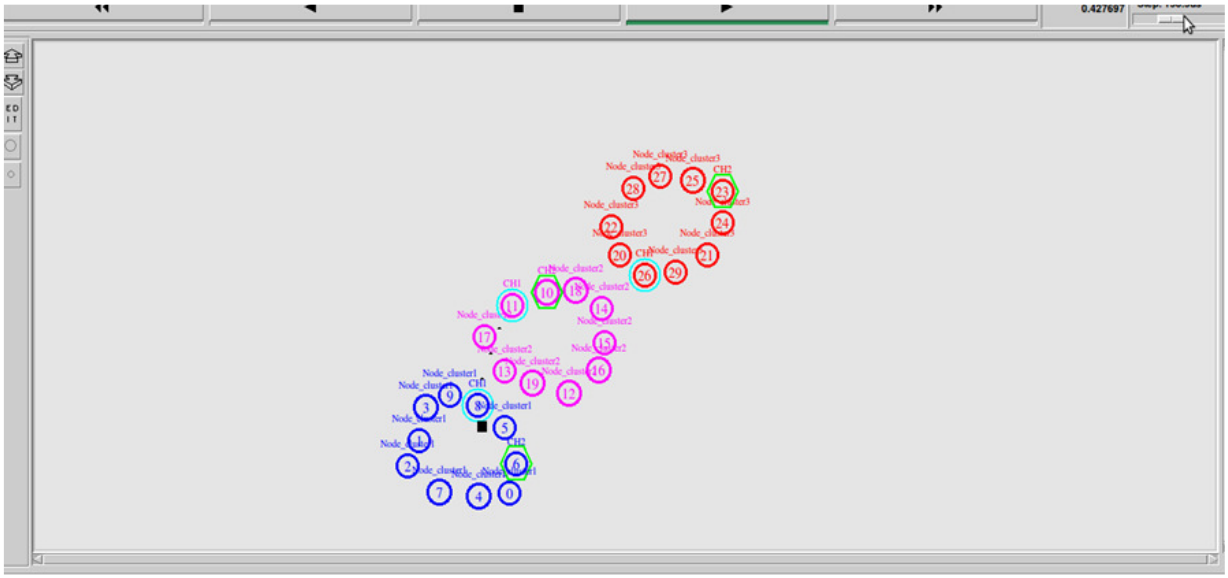

Fig: 2 Dual cluster head Communication

Below fig 3 shows throughput analysis using LEACH and AODV- under Vampire attack. Packet throughput of LEACH is high as compare to AODV under Vampire attack. Under Vampire attack packets are getting dropped whereas under LEACH packets delivery is high.

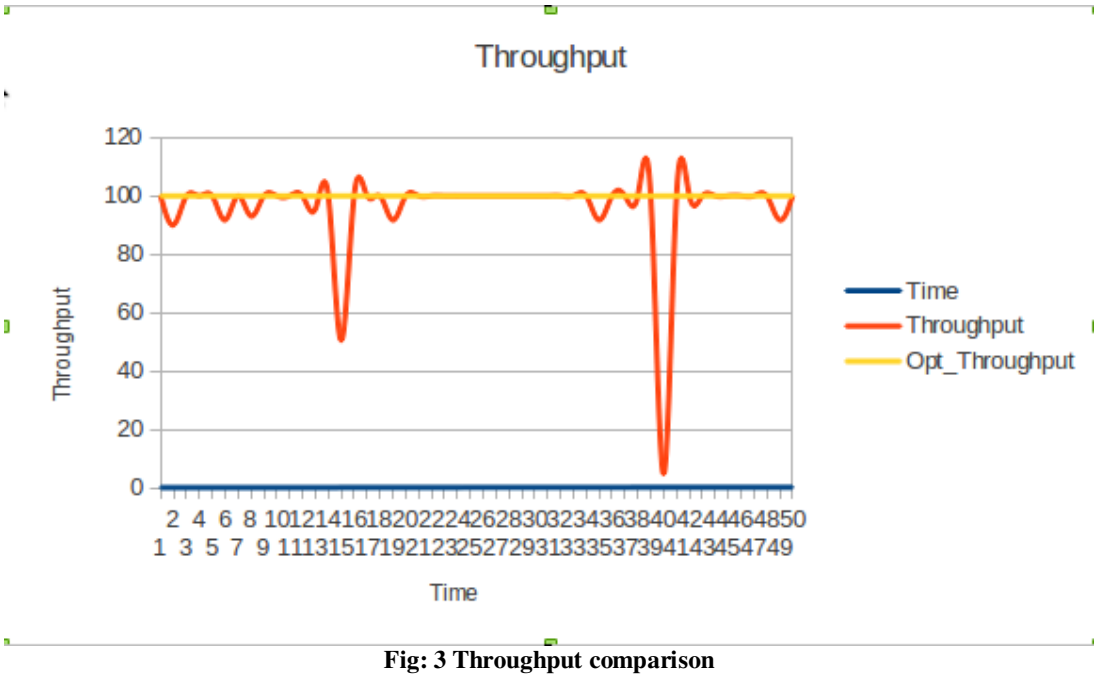

Fig: 3 Throughput comparison

Fig: 4 shows delay comparison with LEACH and under AODV- Vampire attack. Packet delay is less under LEACH as compare to under AODV-vampire attack

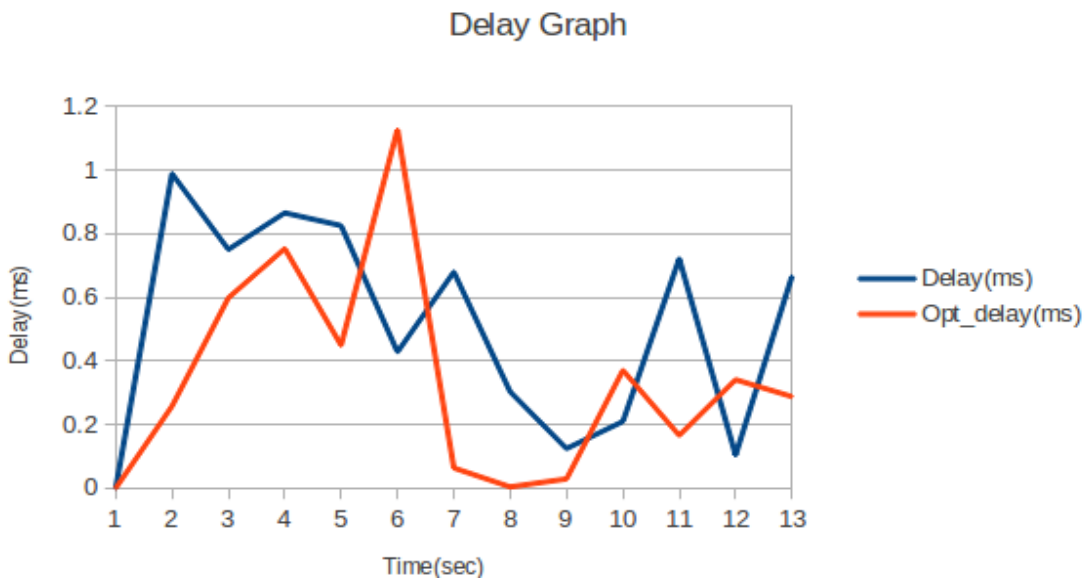

Fig: 4 Delay Comparisons

Energy Comparison

Energy consumes whenever some nodes sends data to other node/base station in WSN. The fig 5 clearly shows that energy consumption is more after vampire attack as compare to LEACH protocol scenario. Attacker node keep sending protocol compliant messages to nodes, which required more energy for communications among nodes and attacker. Whereas less energy consumes in Dual Cluster-Head LEACH communication.

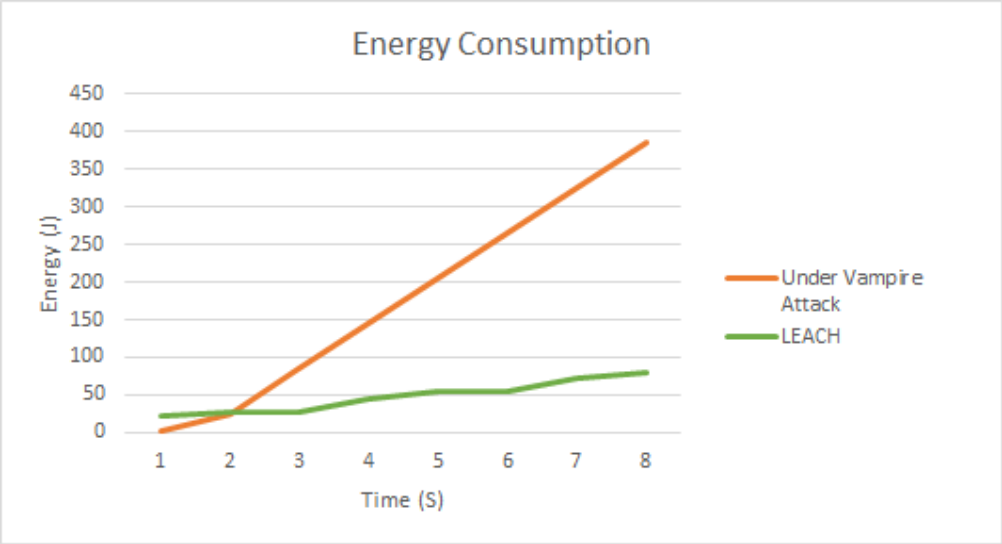

Fig: 5 Energy comparison

IV. CONCLUSIONS

In this paper we studied that the Vampire attacks use routing protocol permanently disable ad-hoc wireless sensor network by depleting nodes battery power. On the basis of LEACH protocol, this paper proposed an energy enhancing algorithm and technique to detect and protect from Vampire attack. The algorithm considers distance factor, residual energy, cluster head selection and strategy of eliminating infected node and attacker from network topology formation. As it is proved in simulation result, the modified algorithm can enhance the node energy efficiently and protect the network from Vampire attack.

V. ACKNOWLEDGMENT

We would like to thanks Department of Computer Science & Engineering and Department of Electronics, RCERT Chandrapur (MS), India, for providing infrastructure and guidance to understand attacks in Wireless sensor networks, Wireless communications.

REFERENCES

[1] Eugene Y. Vasserman and Nicholas Hopper "Vampire attacks: draining life from wireless ad-hoc sensor networks," IEEE Trans on mobile computing vol.12 no.2 year 2013

[2] LinaR.Deshmukh and Amol D. Potgantwar "Prevention of vampire attacks in WSN using Routing Loop," proceedings of IRF International conference, 5th & 6th Feb 2014, Pune India

[3] Susan Sharon George and Suma R "Attack-Resistant Routing for Wireless Ad Hoc Networks," International Journal of CS & IT, vol.5. (3), 2014

[4] A.Vincy, and V.Uma Devi "Maximizing Lifetime of Nodes in Wireless Ad Hoc Sensor Network by preventing Vampire Attack," IEEE International Conference on Innovations in Engineering and Technology, 21st& 22nd Mar 2014

[5] Gowthami.M, and Jessy Nirmal.A.G "Mitigating Vampire Attack in Wireless Ad-Hoc Sensor Networks", IJARCST 2014 Vol. 2. Jan-Mar 2014

[6] Vidya. M and Reshmi.S "Contending Against Energy Debilitating Attacks in Wireless Ad Hoc Sensor Networks'', IJIRAE vol. 1. Mar 2014

[7] Soram Rakesh Singh and Narendra Babu C R "Improving the Performance of Energy Attack Detection in WSN by Secure Forward Mechanism'', International Journal of Scientific and Research Publications, Vol 4, July 2014

[8] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, Ariadne: A secure on-demand routing protocol for ad hoc networks, MobiCom, 2002.

[9] *Anoopa S et al Int. Journal of Engineering Research and Applications ISSN : 2248-9622, Vol. 4, Issue 4(Version 6), April 2014, pp.01-07*

[10] The network simulator- NS-2. http://www.isi.edu/nsname/ns

[11] Manjeshwar A, Grawal D.P. TEEN: A protocol forn enhanced efficiency in wireless sensor networks[c]Proceeding of the 15th Parallel and Distributed Processing Symp. San francisoi, 2001: 2009-2015

[12] Lindsey S, Raghvenda SC. PEGASIS: Power efficient gathering in sensor information systems[c].Proceeding of the IEEE Aerospace Conf. New York, 2002:1125-1130